Об утверждении критериев оценки степени риска в сфере частного предпринимательства в области информатизации, связи, за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи

Утративший силу

Совместный приказ Министра связи и информации Республики Казахстан от 31 августа 2011 года № 263 и Министра экономического развития и торговли Республики Казахстан от 16 сентября 2011 года № 305. Зарегистрирован в Министерстве юстиции Республики Казахстан 17 октября 2011 года № 7262. Утратил силу совместным приказом Министра по инвестициям и развитию Республики Казахстан от 29 июня 2015 года № 735 и и.о. Министра национальной экономики Республики Казахстан от 30 июня 2015 года № 494

Сноска. Утратил силу совместным приказом Министра по инвестициям и развитию РК от 29.06.2015 № 735 и и.о. Министра национальной экономики РК от 30.06.2015 № 494 (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В соответствии с пунктом 4 статьи 13 Закона Республики Казахстан от 6 января 2011 года "О государственном контроле и надзоре в Республике Казахстан", Законом от 11 января 2007 "Об информатизации", Законом от 7 января 2003 года "Об электронном документе и электронной цифровой подписи", Законом от 5 июля 2004 года "О связи", **ПРИКАЗЫВАЕМ**:

1. Утвердить Критерии оценки степени риска в сфере частного предпринимательства:

1) в области информатизации согласно приложению 1 к настоящему совместному приказу;

2) в области связи согласно приложению 2 к настоящему совместному приказу;

3) за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи согласно приложению 3 к настоящему совместному приказу.

2. Комитету связи и информатизации Министерства связи и информации Республики Казахстан (Нуршабеков Р.Р.) в установленном законодательством порядке обеспечить:

1) государственную регистрацию настоящего совместного приказа в Министерстве юстиции Республики Казахстан;

2) после государственной регистрации настоящего совместного приказа его официальное опубликование в средствах массовой информации;

3) опубликование настоящего совместного приказа на официальном интернет-ресурсе Министерства связи и информации Республики Казахстан.

3. Признать утратившим силу совместный приказ Председателя Агентства Республики Казахстан по информатизации и связи от 17 февраля 2010 года № 65 и Министра экономики и бюджетного планирования Республики Казахстан от 19 февраля 2010 года № 88 "Об утверждении критериев оценки степени риска в области информатизации и связи" (зарегистрированный в Реестре государственной регистрации нормативных правовых актов от 24 февраля 2010 года за № 6091, опубликованный в газете "Казахстанская правда" от 13 марта 2010 года № 58-60).

4. Контроль за исполнением настоящего совместного приказа возложить на вице-министра связи и информации Республики Казахстан Сарсенова С.С.

5. Настоящий совместный приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Министр связи и информации Республики Казахстан
_____ *А. Жумагалиев*

И.о. Министра экономического развития и торговли Республики Казахстан
_____ *М. Кусаинов*

Приложение 1
к совместному приказу
Министра связи и информации
Республики Казахстан
от 31 августа 2011 года № 263 и
И.о. Министра экономического
развития и торговли
Республики Казахстан
от 16 сентября 2011 года № 305

Критерии
оценки степени риска в сфере частного предпринимательства в области информатизации

1. Настоящие Критерии оценки степени риска в сфере частного предпринимательства в области информатизации (далее - Критерии оценки степени риска) разработаны в соответствии с Законами Республики Казахстан "О государственном контроле и надзоре в Республике Казахстан" от 6 января 2011 года, "Об информатизации" от 11 января 2007 года и "Об электронном документе

и электронной цифровой подписи" от 7 января 2003 года.

2. Настоящие Критерии оценки степени риска определяют совокупность количественных и качественных показателей риска, на основании которых осуществляется отнесение субъектов информатизации к различным степеням риска.

3. В настоящих Критериях оценки степени риска используются следующие понятия:

1) риск - вероятность причинения вреда в результате деятельности проверяемых субъектов информатизации законным интересам личности, общества, государства, с учетом степени тяжести его последствий при использовании электронных информационных ресурсов и информационных технологий;

2) проверяемые субъекты информатизации (далее - проверяемые субъекты) - собственники и владельцы электронных информационных ресурсов и информационных систем.

4. Критерии оценки степени риска подразделяются на два вида:

1) объективные - основаны на значимости рисков, возможных при осуществлении деятельности проверяемых субъектов;

2) субъективные - определяются в зависимости от допущенных проверяемыми субъектами нарушений установленных требований.

5. Первичное отнесение проверяемых субъектов к группам риска осуществляется на основе объективных критериев оценки степени риска, в зависимости от осуществляемого вида деятельности:

1) к высокой группе риска отнесены - субъекты, осуществляющие деятельность кредитного бюро, а также владельцы контрольно-кассовых машин, являющихся компьютерной системой;

2) к средней группе риска отнесены - субъекты, являющиеся владельцами негосударственных информационных систем, интегрируемых с государственными информационными системами, владельцами электронных информационных ресурсов и информационных систем;

3) к незначительной группе риска отнесены - субъекты, являющиеся поставщиками информации и получателями кредитных историй.

6. Последующее отнесение проверяемых субъектов к группам риска осуществляется с учетом субъективных критериев, к которым относятся грубые, значительные и незначительные нарушения.

7. К грубым нарушениям относятся:

1) отсутствие аттестата соответствия информационной системы требованиям информационной безопасности и принятым на территории Республики Казахстан стандартам;

2) отсутствие обеспечения физической защиты информационных систем с использованием средств защиты информации, в том числе криптографической, а также систем контроля доступа и регистрации фактов доступа к информации;

3) отсутствие обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (к материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

8. К значительным нарушениям относятся:

1) отсутствие исходных программных кодов, инсталляционного пакета и нормативно-технической документации (оригиналов и копий);

2) отсутствие нормативно-технической документации на программные продукты, информационные системы, информационные ресурсы;

3) несоответствие нормативно-технической документации требованиям стандартов.

9. К незначительным нарушениям относится:

1) несвоевременное представление сообщения о снятии с учета в Государственном регистре информационных ресурсов и информационных систем, снятых с эксплуатации по тем или иным причинам или переданных в другое ведомство;

2) несвоевременное представление сообщения о снятии с учета в Депозитарии программных кодов и нормативно-технической документации, снятых с эксплуатации по тем или иным причинам или переданных в другое ведомство;

3) нарушение ежегодной актуализации сведений об электронных информационных ресурсах и информационных систем зарегистрированных в Государственном регистре;

4) нарушение ежегодной актуализации сведений о программных продуктах находящиеся в депозитарии (30 апреля).

10. Определение степени риска и распределение по группам степени риска проверяемых субъектов для осуществления плановых проверок осуществляется ежегодно.

11. Последующее отнесение проверяемых субъектов по группам риска осуществляется на основе анализа результатов предыдущих проверок (за предшествующий год).

12. Проверяемые субъекты, входящие в незначительную группу риска, при совершении в течении проверяемого периода двух и более грубых нарушений или более двух значительных нарушений или более трех незначительных нарушений переводятся в среднюю группу риска.

13. Проверяемые субъекты, входящие в среднюю группу риска, при

совершении в течении проверяемого периода одного и более грубых или двух и более значительных нарушений или более двух незначительных нарушений переводятся в высокую степень риска.

14. При не выявлении последней плановой проверкой нарушений, проверяемые субъекты переводятся в группу меньшей степени риска.

15. Основаниями для приоритетного планирования проверок проверяемых субъектов одной группы риска являются:

1) наибольший непроверенный период (при определении непроверенного периода не берутся в расчет внеплановые проверки);

2) наибольшее количество выявленных грубых и значительных нарушений за прошедший период;

3) наличие наибольшего количества информационных систем и электронных информационных ресурсов.

Приложение 2
к совместному приказу
Министра связи и информации
Республики Казахстан
от 31 августа 2011 года № 263 и
И.о. Министра экономического
развития и торговли
Республики Казахстан
от 16 сентября 2011 года № 305

Критерии оценки степени риска в сфере частного предпринимательства в области связи

1. Настоящие Критерии оценки степени риска в области связи (далее - Критерии) разработаны в соответствии с законами Республики Казахстан "О государственном контроле и надзоре в Республике Казахстан" от 6 января 2011 года и "О связи" от 5 июля 2004 года.

2. Настоящие Критерии определяют совокупность количественных и качественных показателей риска, на основании которых осуществляется отнесение субъектов в области связи к различным степеням риска.

3. В настоящих Критериях используются следующие понятия:

1) риск - вероятность причинения вреда в результате деятельности Субъектов в области связи законным интересам физических и юридических лиц и государства, общества с учетом степени тяжести его последствий, а именно:

бесконтрольное использование платного ограниченного ресурса радиочастотного спектра, которое может привести к недопоступлению

обязательных платежей в государственный бюджет;

использование радиочастотного спектра без разрешительных документов, которое может привести к возникновению радиопомех и невозможности использования его законными владельцами;

эксплуатация оборудования на сетях телекоммуникаций без технических средств проведения специальных оперативно-розыскных мероприятий, которая может привести к невозможности проведения органами оперативно-розыскной деятельности необходимых мероприятий;

2) субъект контроля - оператор связи (физическое или юридическое лицо, получившее лицензию на предоставление услуг связи); хозяйствующие субъекты , осуществляющие деятельность в области связи (операторы связи, владельцы специальных, ведомственных и корпоративных сетей телекоммуникаций, отдельного коммутационного оборудования, подключаемого к сети телекоммуникаций общего пользования, владельцы радиоэлектронных средств, являющиеся пользователями радиочастотным спектром).

4. Отнесение субъектов контроля к степени рисков осуществляется в два этапа:

первый этап - на основании объективных критериев степени риска;

второй этап - на основании субъективных критериев степени риска.

5. Объективные критерии степени риска:

1) к высокой степени группы риска отнесены - субъекты, получившие лицензии на предоставление следующих услуг связи: междугородная, международная, сотовая; а также местная и передача данных имеющих радиочастотный спектр для предоставления услуг связи;

2) к средней степени группы риска отнесены - субъекты, получившие лицензии на предоставление следующих услуг связи: передача данных, IP-телефония, местная посредством проводной связи, телекоммуникации по выделенной сети связи, спутниковая подвижная связь, мобильная телекоммуникационная связь, предоставление каналов связи;

3) к незначительной степени группы риска отнесены - хозяйствующие субъекты, использующие радиочастотный спектр в производственных целях.

6. Субъективные критерии оценки степени риска подразделяются на:

грубые нарушения;

значительные нарушения;

незначительные нарушения.

7. К грубым нарушениям относятся:

1) предоставление услуг связи без соответствующей лицензии;

2) использование радиочастотного спектра без соответствующего разрешения ;

3) использование ресурса нумерации без соответствующего разрешения либо нарушение принципа нумерации;

4) отсутствие технических средств проведения специальных оперативно-розыскных мероприятий (далее - ОРМ) на телекоммуникационном оборудовании и нарушение обязательств по сбору и хранению служебной информации об абонентах, для обеспечения ОРМ.

8. К значительным нарушениям относятся:

1) использование не сертифицированного оборудования;

2) эксплуатация радиоэлектронных средств и высокочастотных устройств без разрешения на эксплуатацию;

3) нарушения порядка присоединения к сети телекоммуникаций общего пользования;

4) не соблюдение условий действия лицензий, а также несоответствие установленным квалификационным требованиям операторов связи;

5) не продление сроков действия разрешения на использование радиочастотного спектра;

6) отсутствие регистрации радиоэлектронных средств и высокочастотных устройств;

7) Несоответствие эксплуатационно-технических характеристик РЭС и ВЧУ данным, указанным в разрешениях на использование радиочастотного спектра и на эксплуатацию РЭС и ВЧУ;

8) отсутствие метрологической базы (внесенной в реестр государственной системы измерения Республики Казахстан) для проведения контрольно-измерительных и испытательных работ (принадлежащей заявителю на правах собственности либо аренды при условии наличия соответствующего договора).

9. К незначительным нарушениям относится:

1) не продление сроков действия разрешения на эксплуатацию на радиоэлектронное средство и высокочастотное устройство;

2) отсутствие разрешений на приобретение радиоэлектронных средств и высокочастотных устройств, в случае приобретения их на территории Республики Казахстан;

3) не предоставление следующей информации о:

территории, на которой предоставляются услуги, по этапам создания и/или развития сети телекоммуникации с привязкой к административно-территориальному делению Республики Казахстан;

степени самостоятельности во взаимоотношениях с потребителями услуг (осуществляется самостоятельно или требуются посредники - "поставщики услуг") ;

используемых стандартах и протоколах при строительстве типа сети;
емкости сети, в том числе по этапам создания и/или развития;
наличии схемы организации связи в привязке к административным пунктам создания сети;
взаимодействии с сетью телекоммуникаций общего пользования, другими сетями связи на территории Республики Казахстан;
способах организации межстанционных соединений (по собственным средствам сети связи заявителя с указанием конкретных технических средств, по арендованным каналам других сетей);
наличии системы учета трафика;
праве владения, пользования, распоряжения средствами связи (на правах собственности либо на правах аренды);
использовании аппаратуры повременного учета стоимости местных телефонных соединений, аппаратуры определения номера (требование для операторов связи, осуществляющих деятельность по предоставлению услуги местной телефонной связи);
порядке предоставления услуг почтовой связи (в случае предоставлении услуги почтовой связи);
порядке предъявления на таможенный досмотр международных почтовых отправлений (в случае предоставлении услуги почтовой связи).

10. Определение степени риска и распределение по группам степени риска субъектов в области связи для осуществления плановых проверок будет осуществляться ежегодно.

11. Распределение субъектов в области связи по степени риска будет осуществляться на основе анализа по результатам предыдущих проверок (за предшествующий год).

12. Субъекты контроля, входящие в незначительную степень риска, при совершении в течении проверяемого периода до двух грубых или более двух значительных нарушений переводятся в среднюю степень риска, а при совершении трех грубых нарушений - в высокую степень риска.

13. Субъекты контроля, входящие в среднюю степень риска, при совершении в течении проверяемого периода одного и более грубых или двух и более значительных нарушений переводятся в высокую степень риска.

14. При невыявлении последней плановой проверкой нарушений, субъекты регулирования переводятся в группу незначительной степени риска.

15. Субъекты высокой или средней группы риска в зависимости от соблюдения требований норм законодательства в области связи будет переводиться из одной группы в другую и, соответственно, будет меняться периодичность их проверки.

16. Отбор субъектов внутри одной степени риска осуществляется уполномоченным органом в области связи следующим образом:

1) наибольший непроверенный период (при определении непроверенного периода не берутся в расчет внеплановые тематические проверки);

2) степень тяжести выявленных нарушений за прошедший период;

3) наличие наибольшего количества радиоэлектронных средств.

Приложение 3
к совместному приказу
Министра связи и информации
Республики Казахстан
от 31 августа 2011 года № 263 и
И.о. Министра экономического
развития и торговли
Республики Казахстан
от 16 сентября 2011 года № 305

Критерии
оценки степени риска в сфере частного предпринимательства за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи

1. Настоящие Критерии оценки степени риска в сфере частного предпринимательства за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи (далее - Критерии оценки степени риска) разработаны в соответствии с законами Республики Казахстан "О государственном контроле и надзоре в Республике Казахстан" от 6 января 2011 года, "Об информатизации" от 11 января 2007 года и "Об электронном документе и электронной цифровой подписи" от 7 января 2003 года .

2. Настоящие Критерии оценки степени риска определяют совокупность количественных и качественных показателей риска, на основании которых осуществляется отнесение субъектов информатизации к различным степеням риска.

3. В настоящих Критериях оценки степени риска используются следующие понятия:

1) риск - вероятность причинения вреда в результате деятельности проверяемых субъектов законным интересам личности, общества, государства, с учетом степени тяжести его последствий при использовании электронных документов и электронной цифровой подписи;

2) проверяемые субъекты (далее - проверяемые субъекты) - удостоверяющие центры;

3) удостоверяющий центр - юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства.

4. Критерии оценки степени риска подразделяются на два вида:

1) объективные - основаны на значимости рисков, возможных при осуществлении деятельности проверяемых субъектов;

2) субъективные - определяются в зависимости от допущенных проверяемыми субъектами нарушений установленных требований.

5. Первично все проверяемые субъекты относятся к высокой группе риска.

6. Последующее отнесение проверяемых субъектов к группам риска осуществляется с учетом субъективных критериев, к которым относятся грубые, значительные и незначительные нарушения.

7. К грубым нарушениям относятся:

1) отсутствие сертифицированных средств криптографической защиты информации для аппаратно-программного комплекса удостоверяющего центра;

2) отсутствие свидетельства об аккредитации удостоверяющего центра;

3) отсутствие аппаратно-программного комплекса, необходимого для осуществления заявленного вида деятельности;

4) отсутствие сертификата соответствия на используемые СКЗИ по СТ РК 1073-2007, которые применяется в данном удостоверяющем центре и его пользователями.

8. К значительным нарушениям относятся:

1) отсутствие технических помещений для размещения и эксплуатации программно-аппаратных средств удостоверяющего центра;

2) отсутствие лицензии на реализацию (в том числе иной передаче) средств криптографической защиты информации;

3) отсутствие разрешения на проведение работ с использованием сведений, составляющих государственные секреты Республики Казахстан, выдаваемого органами национальной безопасности Республики Казахстан, или заключенного в установленном законодательством порядке договора на выполнение совместных секретных работ;

9. К незначительным нарушениям относится:

1) отсутствие квалифицированного инженерно-технического персонала не менее трех человек, отвечающих соответствующему профессиональному уровню и имеющих стаж работы в соответствии с квалификацией не менее 3-х лет, а также документов подтверждающих соответствие удостоверяющего центра

квалификационным требованиям (дипломы, сертификаты и иного рода свидетельства о присвоении квалификации соответствующей профилю деятельности удостоверяющего центра);

2) отсутствие схемы взаимодействия модулей (компонент) удостоверяющего центра и схемы электронной цифровой подписи с данными о применяемых алгоритмах криптографических преобразований и другими исходными данными (основными требованиями) по реализации процесса формирования электронной цифровой подписи и требованиями к отдельным параметрам и удостоверяющему центру, утвержденные заявителем;

3) отсутствие утвержденных нормативно-технических документов, согласно подпункту 6) пункта 5 Правил проведения аккредитации удостоверяющих центров, утвержденных Постановлением Правительства Республики Казахстан № 1222 от 19 ноября 2010 года;

4) наличие фактов некорректной работы функционирующего программного обеспечения, реализующего функции электронной цифровой подписи.

10. Определение степени риска и распределение по группам степени риска проверяемых субъектов для осуществления плановых проверок осуществляется ежегодно.

11. Последующее отнесение проверяемых субъектов по группам риска осуществляется на основе анализа результатов предыдущих проверок (за предшествующий год).

12. Проверяемые субъекты, входящие в незначительную группу риска, при совершении в течении проверяемого периода одной и более грубых нарушений или более двух значительных нарушений или более трех незначительных нарушений переводятся в среднюю группу риска.

13. Проверяемые субъекты, входящие в среднюю группу риска, при совершении в течении проверяемого периода одного и более значительных нарушений или более двух незначительных нарушений переводятся в высокую степень риска.

14. При не выявлении последней плановой проверкой нарушений, проверяемые субъекты переводятся в группу меньшей степени риска.

15. Основаниями для приоритетного планирования проверок проверяемых субъектов одной группы риска являются:

1) наибольший непроверенный период (при определении непроверенного периода не берутся в расчет внеплановые проверки);

2) наибольшее количество выявленных грубых и значительных нарушений за прошедший период.